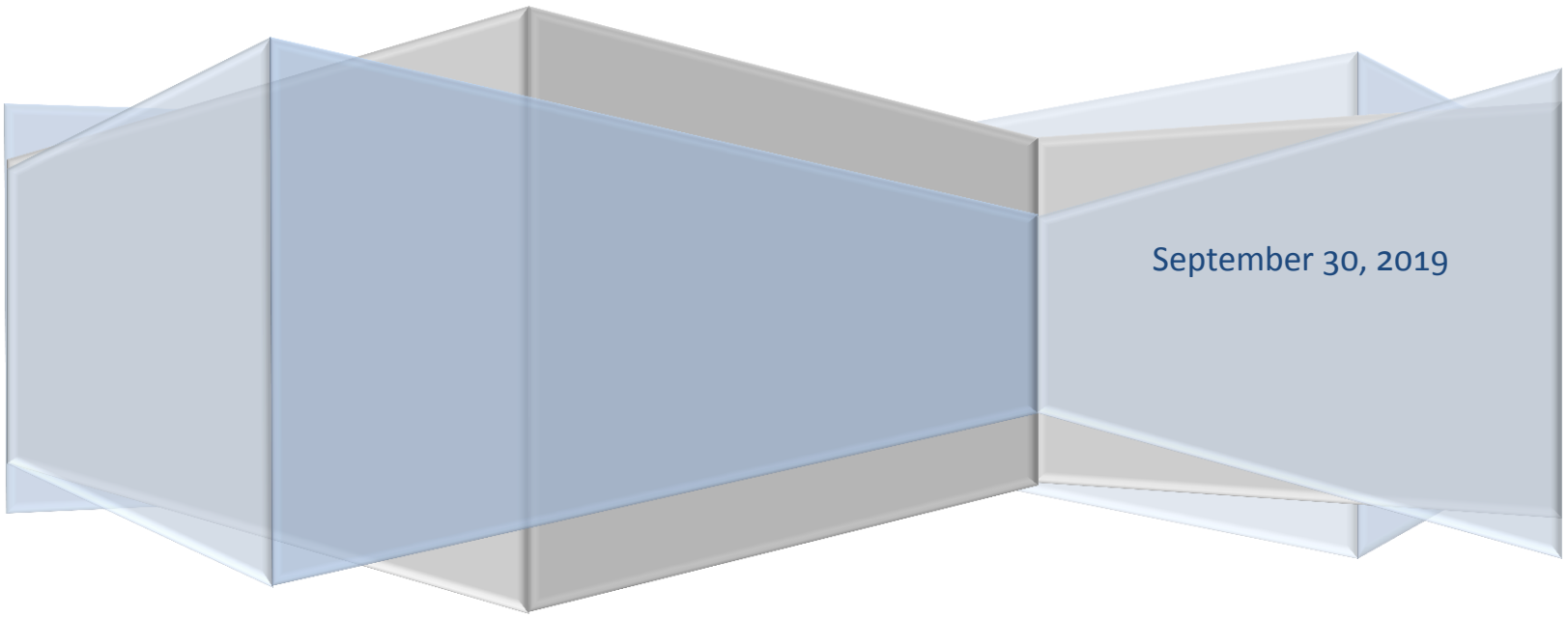
VOTER GA
Voters Organized for
Trusted Election Results in Georgia

Unresolved Security Threats for Ballot Marking Devices

A general guide to BMD verifiability, auditability, privacy and preparation security threats

Garland Favorito



September 30, 2019

Table of Contents

Abstract 2
About the Author 3
The Sunset of DREs 4
BMD Overview 5
BMD Election System Integration Points 6
BMD Ballot Format Quality 7
Completeness 7
Clarity 8
Independence 8
BMD Product Quality Map 9
BMD Threat Models 10
All-in-One Security Threat 10
ADA Selection Summary Privacy Threat 11
Bar-Coded Data Security Threat 12
Bar-Coded Vote Verifiability Threat 13
Selection Summary Auditability Threat 14
BMD Malfunction Audit Threat 15
Dropped Race Threat Model 17
A Real Life Dropped Race Undervote Anomaly 18
Targeted Race Concealment 21
Election Preparation Security Threat 23
BMD Policy Conclusions 26
BMD Audit Weaknesses 26
Recommended BMD Evaluation Policies 27
Appendix 28
References 31
Voting System Evaluation Tools 30

Abstract

Some jurisdictions in different states have begun transitioning their voting equipment to electronic ballot marking devices (BMD). While these devices are necessary for disabled voter accessibility and Americans with Disability Act (ADA) compliance, some jurisdictions are requiring these touchscreen ballot printers to be used for all voters. Since most margins of victory exceed the number of disabled voters it is improbable that disabled voter BMDs can be hacked to rig an election. However, the attempt to use BMDs for additional voters creates a severe threat of election rigging that must be properly mitigated.

The move toward BMDs has generated a series of discussions, papers and articles among computer scientists and election integrity advocates that define BMD security vulnerabilities and debate whether or not they can be adequately alleviated. This paper adds new information to the discussion in several ways:

- It outlines key attributes of BMDs that determine BMD ballot quality and maps currently available vendor products to those attributes.
- It discusses the different security threats that are unique to those attributes, including threats to privacy, verifiability, auditability and overall security.
- It includes real-life, unmitigated examples of security threats identified in Georgia's voting systems.
- It details a new threat model that has not previously been analyzed.
- It provides evidence the new "Dropped Race Threat Model" may have already been implemented in a statewide 2018 Georgia race.

Jurisdictions must make genuine efforts to analyze BMD purchases more thoroughly and protect the constitutional rights of their voters against these various security threats. Those rights are implicit in Art. I Sec. IV and confirmed by U.S. Supreme Court decisions such as *Reynolds v. Sims* (1964) in which the court declared: *"the right to have a vote counted is as open to protection as the right to put a ballot in a ballot box".*

Likewise, voters who have no mechanism to ensure their votes were counted as cast are equally as disenfranchised as voters who have no mechanism to determine if their ballots were placed in a ballot box.

About the Author

Garland Favorito was the **first technology professional in America** to advocate against a statewide implementation of paperless electronic voting on the grounds that it poses a threat to the Constitutional right to vote. In February of 2002, he sent written warnings to election officials explaining how paperless voting produces results that cannot be verified by the voter or audited by elections officials.[i] His February 2002 emails to Professor. Britain Williams, who headed the Georgia voting system implementation and Assistant Secretary of State Michael Barnes, were authenticated by both parties under oath in depositions. Those depositions were part of the *Favorito v. Handel* court case that was decided by the Georgia Supreme Court. In 2017, two dozen computer scientists wrote to the Georgia secretary of state urging him to abandon electronic voting for essentially the same reasons Garland had provided 15 years earlier.

After his advice was ignored, Garland founded *Voters Organized for Trusted Election Results in Georgia* (VoterGA). He also serves as a volunteer Elections Director for the Constitution Party of Georgia. VoterGA is a nonpartisan, non-profit, all-volunteer organization dedicated to restoring the integrity of Georgia elections. Its primary objective is to advocate for verifiable, auditable and recount-capable voting in Georgia. It also advocates for fair and equal ballot access for all Georgia candidates.

Garland makes presentations for VoterGA to a wide range of groups throughout the state and is recognized as a leading expert on the usage of, and risks involved with, Georgia's voting machines. He has testified in numerous committee hearings, produced a variety of reports, and was deposed for over six hours in the *Favorito v. Handel* lawsuit.

Garland is a career Information Technology (IT) professional with over 40 years of in-depth experience in internet systems design, business systems analysis, database administration, application development, systems architecture, life cycle methodologies, computer programming, project management, and multi-factor security. His experience centers on medium and large-scale mission-critical applications in nearly all facets of American business. His industry experience includes banking, financial systems, health care, accounting, manufacturing, inventory, purchasing, retailing, utilities, telecommunications, insurance, software development and the service industry.

Contact Info:
Garland Favorito
VoterGA Co-founder
garlandf@voterga.net
garlandf@msn.com
404 664-4044

The Sunset of DREs

Since their inception, Direct Recording Electronic (DRE) voting machines have been riddled with inherent design flaws. Paperless DREs are unable to produce results that can be verified by the voter, audited by elections officials or recounted for candidates. A U.S. District Court recently banned this type of machine from further use in Georgia elections because its flaws impair the constitutional right of voters.

Specifically, paperless DREs cannot support the three most critical election functions within their operational scope:

- Voters cannot verify the selections they made are recorded internally on computer media;
- Election officials have no mechanism to audit the counts accumulated and published by the system to ensure they are accurate;
- Candidates cannot receive a true recount because the machines can only reprint previous unverifiable results.

Paperless DREs are extremely vulnerable to a variety of hacking techniques as explained in many academic- and state-commissioned studies such as Princeton's *Security Analysis of the Diebold AccutVote-TS Voting Machine* as demonstrated by Dr. Ed Felten before the U.S. House Administration Committee. These blatant design flaws of paperless DREs render fraud and errors undetectable in elections for which they are used.[ii]

Since paperless DRE voting machines generally cannot support these three most critical election functions, they have never been suitable to conduct elections. Nevertheless, many of the machines received federal and state certifications and many jurisdictions throughout the country subsequently purchased them under questionable circumstances without truly assessing the security risks involved.

In 2002, the Georgia General Assembly removed an audit trail law to clear the way for purchasing paperless DREs. The 2002 DRE results produced controversial upsets in the race for Governor and U.S. Senate. Britain Williams acknowledged under oath in deposition that the systems received software patches before the election and was not recertified as required by law.[iii]

In response to the issues, some vendors incorporated a Voter Verified Paper Audit Trail (VVPAT) into their equipment. VVPAT machines print voter selections on a paper slip behind glass so the voter can see their selections. Once the voter reviews their selections and formally casts their "ballot" the machine deposits the "ballot" in a secure ballot box. But in lieu of an actual ballot, VVPAT machines typically show Selections Summaries on small slips of paper and embed the votes to be accumulated in an unverifiable bar code on the paper, which typically contains a continuous roll of cast "ballots".

Such VVPAT output is fraught with problems. Continuous rolls are plagued by jams, smears, tears and cumbersome audit procedures. Studies referenced in this paper have shown that voters do not spend time to verify Selection Summaries and votes embedded in bar codes are totally unverifiable to the voter. Therefore, VVPAT severely impairs verifiability and auditability of election results.

BMD Overview

As the problems with paperless DREs became more widely documented and understood, jurisdictions turned to electronic Ballot Marking Devices (BMDs) as an alternative technology in lieu of VVPAT. However, these jurisdictions tend to ignore the reality that both BMDs and DREs have similar deficiencies and threat vulnerabilities.

A BMD allows a voter to employ a touchscreen to mark a ballot, which the voter then inserts into a scanner that stores the ballot in a secure ballot box and begins the process of accumulating the votes. BMDs have several advantages:

- They store ballot templates that can be produced for the voter on demand at time of voting;
- They utilize a touchscreen interface to allow voters to make selections;
- They produce a paper trail for use in audits and recounts;
- They mark all ballots consistently for all voters;
- They can be equipped with audio devices to support voters with disabilities such as visual impairment.

However, all BMDs are not created equal. A variety of jurisdictions have begun purchasing BMDs for all voters without realizing some have flaws similar to those of paperless DREs. Any voting system acquisition should include tasks that:

- Assess and plan for the mitigation of security threats against electronic components.
- Evaluate the pros and cons of BMD, Ballot on Demand (BOD) and pre-printed hand marked paper ballot (HMPB) solutions.
- Assess the costs of BMD, BOD and HMPB system alternatives.
- Document the conclusions reached by the evaluation.

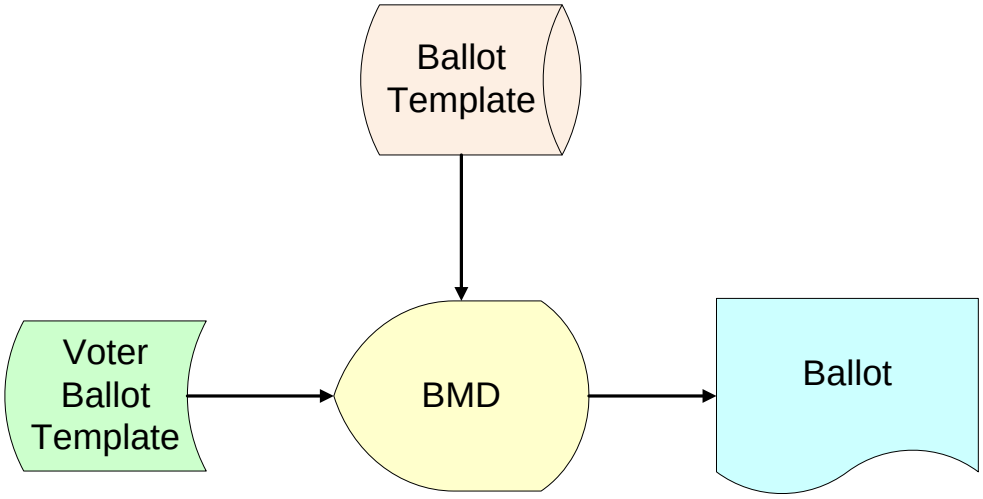
All BMDs are vulnerable to certain security threats that, left unmitigated, render them **inappropriate for use** by the general populace. Professors Andrew Appel, Richard Demillo and Phillip Stark explain that any voting system must produce results that are defensible and contestable. In other words, if the BMD produces correct results, it must supply ample evidence to prove the results are correct to the average voter. If the BMD produces incorrect results, there must be a means to challenge the results and apply an appropriate remedy.[iv]

The abilities to defend and contest election results are paramount to identifying and mitigating security threats. BMDs can receive and transmit threats through their integration points with the election management system. The quality of the ballot format a BMD produces can at least partially influence the ability of the election system to withstand security threats.

BMD Election System Integration Points

BMDs typically have three security impacting integration points with the overall election management system as shown:

- They receive ballot definition templates from an election preparation system in advance of their use in voting;
- They receive a voter ballot template and authorization to cast a vote from a voter check-in system at time of voting;
- They produce a paper trail with voter selections once a voter has made their selections electronically;



The ballot definition templates are files that are preloaded into each BMD by county elections personnel. The voter ballot template is typically a voter access card or bar coded paper with a ballot template ID that tells the election management system the voter is authorized to cast one vote. The bar coded paper serves the same purpose for many BMDs that the voter access cards server for DREs

The voter registration system authenticates the voter and produces the paper or updates a card for a poll worker to hand to the authenticated voter. That voter then takes the card or paper to the BMD which reads it and displays the correct ballot template for the voter.

Once authenticated with the correct ballot template, the voter can use the BMD to make selections only since the BMD should not have an integrated tabulator. After completing their selections the voter can then request to print a paper trail commonly referred to as a "ballot" and insert it into the scanner for permanent recording, subsequent tabulation and general safekeeping.

The scope of this paper focuses on these integration points and the related internal BMD operational characteristics that may impact voting security.

BMD Ballot Format Quality

The attributes of a ballot that a BMD produces significantly impact its verifiability, auditability, privacy and security capabilities. The following attributes are suggested to help quantify BMD ballot format quality:

- **Completeness** – Does the BMD produce a full ballot in the same style and format of mail-in ballots and hand marked paper ballots or does it merely list voter selections on a piece of paper?
- **Clarity** – Does the BMD produce a transparent ballot containing only human readable data and alignment marks or does it also have cryptic, encoded data that cannot be understood by the voter?
- **Independence** – Is the BMD a stand-alone device that produces a ballot independently of other election equipment or does it contain integrated components such as a scanner and accumulator?

These attributes can be further broken down into the following characteristics:

Completeness

Ballot completeness is necessary to establish consistency in the format and content for a given ballot template across different voting methods. These voting methods are for:

- Mail-in;
- Early voting;
- Election Day;
- Provisional voters;
- Disabled voters.

BMDs produce the choices made by the voter in two different ways:

  - **Full Ballot** – The BMD ballot contains all selected candidates, unselected candidates and all referendum language in a manner that is similar in style and appearance to a corresponding mail-in ballot or hand marked paper ballot.
  - **Selection Summary –** The BMD ballot contains text only for the selections chosen by the voter including a “Yes” or “No” for referendum votes.

A full ballot provides better, verifiability, auditability and privacy through complete and consistent balloting. Selection summaries have significant auditing and verifiability problems described in subsequent sections.

Clarity

Ballot clarity for the voter is necessary to ensure that the voter can verify their selections properly. Different BMDs have different degrees of clarity for their paper-trail characteristics. These characteristics can be identified as:

- **Transparent** – The BMD ballot contains only text, alignment marks and mark sense bubbles that are visible to the voter and interpreted by the scanner;
- **Bar Coded Data** – The BMD ballot contains a bar code with generic information such as Election ID and Precinct ID but the bar code contains no votes;
- **Bar Coded Votes** – The BMD embeds the votes in a barcode that the scanner uses to accumulate the ballot votes.

BMDs that produce fully transparent ballots provide better security and verifiability. Bar codes reduce security. Bar coded votes further reduce security by eliminating verifiability for the voter altogether.

Independence

BMD functional independence is necessary to properly isolate, secure and audit different election functions. There are two general types of BMD units that have independence differences. They are:

- **Stand-alone** – The BMD performs no other election functions besides allowing voters to mark their ballots.
- **All-in-One** – The physical unit of the BMD also contains a scanner and possibly an accumulator in addition to the ballot marker.

Stand-alone BMD units provide the best security. All-in-one BMD units with integrated scanners and accumulators compromise verifiability, auditability and security.

BMD Product Quality Map

Current vendor BMD products tend to map onto the previously defined characteristics of the BMD attributes roughly as follows:

		Completeness			Clarity				Independence	
BMD	Vendor	Full Ballot	Selection Summary		Transparent	Bar Coded Data	Bar Coded Votes		Stand Alone	All in One
AutoMark	ESS	✓			✓				✓	
Clear Access	Clear Ballot	✓			✓				✓	
COTS-BMD	Avante	✓				O			✓	
Express Vote	ES&S		X				X		O	
Express Vote XL	ES&S		X				X			X
Image Cast Evolution	Dominion	✓			✓					X
Image Cast X	Dominion		X				X		✓	
Open Elect OVI	Unisyn		X				X		✓	
A4-600	Smartmatic		X			O			✓	
Verity Duo	Hart Intercivic		X			O			✓	
Verity Touch Writer	Hart Intercivic	✓			✓				✓	

These mapping characteristics are based on demonstrations, specifications and communications from vendors and evaluators. They are subject to change if vendors upgrade their products while retaining the same product name.[1]

1. COTS-BMD and Verity Duo have bar coded data but not bar coded votes
2. A4-600 has bar coded votes that are not tabulated
3. Express Vote has an integrated tabulator but can be configured as disabled

BMD Threat Models

All-in-One Security Threat

Most BMDs are stand-alone devices that mark ballots for voters. This separation of election functions generally improves security by isolating components in a manner in which security controls can be properly applied.

However, a few BMDs referred to in this paper as "All-in-One" BMDs contain a scanner and a ballot marking device all in one physical unit. These devices present an additional security threat. Since the marking device and scanner are combined into one paper path, the device can actually add votes to a ballot after a voter reviews the ballot selections and inserts the ballot into the scanner for casting. The device could also undetectably spoil votes that voters intend to cast if it adds overvotes or extraneous marks to the ballot after the voter inserts it.

In his September and October 2018 articles, Professor Appel amply pointed out the deficiencies of two different All-in-One BMDs. He also explained that they have an even more dangerous auto-cast feature that allows voters to bypass the ballot review and verification process altogether. He dubbed this feature as a *"permission to cheat"* because it gives the computer a no risk opportunity to alter the ballot after the voter declares their intention to not review. [v] [vi]

Voting systems must be software and hardware independent to detect fraud. This concept is explained by several authors such as Ron Rivest and John Wack and it is incorporated into the Election Assistance Commission's Voluntary Voting System Guidelines (VVSG 2.0)[vii]

An "All-in-One" BMD provides the capability for a hacker to easily implement a "Vote Swapping Threat Model" to shift votes from one candidate to another and rig election results of a specific race. Therefore, "**All-in-One" BMDs are unacceptable devices to use to conduct elections.**

ADA Selection Summary Privacy Threat

BMDs are almost unanimously recognized as beneficial to disabled voters and being uniformly in compliance with the American's for Disabilities Act (ADA). Their supplemental audio devices and hand controllers make voting much more independent for voters with disabilities such as visual impairments.

However, not all BMDs are suitable for use by disabled voters. Disabled **voters are entitled to the same ballot secrecy protections as other voters** who cast hand marked paper ballots at the polls. Since the volume of disabled voters is extremely low at any precinct, it would be relatively easy to identify the ballot cast for a specific disabled voter if that ballot template was significantly different from hand marked paper ballots that are being used at the polling location.

This problem arises when jurisdictions fail to purchase BMDs that produce a full ballot with a similar ballot format for disabled voters as used by other voters. BMDs that produce a Selection Summary are not suitable to protect privacy for disabled voters in jurisdictions that are using hand marked paper ballots for all other voters.

Furthermore, disabled voters and their assistants should also not suffer a loss of ballot verifiability. **When a disabled voter chooses to be accompanied by an assistant, that assistant should be able to fully verify the paper ballot to be cast if the disabled voter chooses for the assistant to do so.** The assistant must be able to verify the ballot in the same manner as other voters would verify their ballots. If a BMD embeds votes in a bar code, the assistant will have no way to verify those votes and the disabled voter would be forced to rely only on the marking audio component for verification and not the actual ballot itself. If other voters use transparent hand marked paper ballots that have no bar codes then disabled voters must be allowed to record their votes on a similar type of ballot.

To circumvent these inconsistencies, some jurisdictions are attempting to force *all* voters to vote on BMDs that embed bar coded votes into an unverifiable Selection Summary. This approach is an excessively expensive alternative that can triple the costs of a voting system implementation and double the costs of ongoing expenses as shown in the 2019 VoterGA estimates for Georgia in the Appendix. But more importantly, it gives hackers **a golden opportunity to rig elections** in those jurisdictions.

Since the volume of disabled voters is extremely low, it would be almost impossible to rig an election by manipulating disabled voter ballots only. However, implementing an unverifiable system for all voters is an invitation to fraud through a 'Vote Swapping Threat Model" that could alter any election. All voters should no more be required to use this type of BMD than they would be required to use handicap access ramps that assist disabled individuals in entering buildings.

Even if Selection Summaries do not contain bar-coded votes their reduced auditability poses additional threats that render them undesirable for use by all voters. These verifiability and auditability threats will be described in subsequent sections. In summary, **BMDs for disabled voters must have the capability to produce a transparent, full ballot to ensure privacy, verifiability and consistency for disabled voters**.

Bar-Coded Data Security Threat

Bar-coded BMD ballots present security challenges not present in transparent ballots even when the bar code may not have embedded votes.

Transparent ballots contain no data. They use alignment marks to communicate with the scanner. The scanner uses those marks as reference points to orient the ballot so that it can interpret the mark-sense bubbles for the corresponding text selections made by the voter. Since the ballot contains no data it cannot be corrupted.

Some BMDs produce ballots that contain rectangular bar codes or square QR codes that can contain a significant amount of data. For elections, these coded ballots contain data such as Election ID and Precinct ID. It is generally unnecessary to code this election data since the scanner could be programmed to read the clear, plain text for the data instead.

Bar-coded ballots present a security risk for conducting elections. A bad actor that had access to election preparation files could program the BMD to inject nefarious instructions into the bar code and program the scanner to recognize those instructions and record the votes for candidates differently from what the text selections showed the voter. This can be achieved with little chance of detection by election officials.

This threat could possibly be managed with different types of procedures to verify ballot content at voting locations. For example, election officials could selectively use a bar code reader to confirm that ballot bar codes contain no nefarious instructions. However, many jurisdictions that use a ‘”Bar Coded Data” BMD have no such procedures. Therefore, a pure transparent ballot is more desirable to eliminate this security threat and protect the ballot against potential corruption.

Bar-Coded Vote Verifiability Threat

One of the most fundamental principles in conducting elections is that a voter must be able to verify the votes on their ballot that will be recorded and accumulated into election results. However, several newer BMDs cannot even fulfill this simple principle of ballot clarity.

These "Bar-Coded Vote" BMDs record embedded votes in bar codes that the voter cannot verify. The scanner then reads the votes in the bar code and uses them for the accumulation rather than using the mark sense bubbles for the text selections the voter can actually see. The data structure in the bar code is proprietary property of the vendor so the data is not available to decode. In addition, one or more vendors encrypt the bar code making it close to impossible to decode.

Defenders of these unverifiable BMDs sometimes claim that auditing can compensate for such a glaring design deficiency. This argument fails for a variety of reasons:

- Only a small percentage of election ballots would be audited with a Risk Limited Audit protocol and that percentage depends upon the margin of victory; thus, the vast majority of ballots, typically 90-99%, would remain unverifiable, not audited and vulnerable to election rigging.
- Risk Limiting Audits, while considered state of the art in auditing today, can typically only provide a 90% or so chance of detecting election rigging.
- Election insiders can easily compromise the randomizing of audit race selection or tamper with ballots to be audited so only correctly recorded ballots are reviewed by auditors while remaining ballots are vulnerable to election rigging in a similar manner to the tampering in the 2004 Cuyahoga County, Ohio U.S. Presidential recount. [viii]
- Election audit procedures and legal requirements are inadequate or non-existent in many states and cannot protect voters against election rigging.
- Some states have little or no experience in conducting audits since they have used paperless DREs producing results that cannot be audited.
- When audits uncover potential hacking, the revelation is so politically sensitive that election officials refrain from disclosing them or pursuing further investigation.
- Unlike verifiability that can identify problems during testing, audits identify problems only after an election is conducted; thus, the only remedy is a new election, which may be politically unpalatable and subject to legal challenge.

"Bar Coded Vote" BMDs also suffer further from auditability issues described in subsequent sections. There is simply no substitute for direct verifiability of a ballot by the voter. **Unverifiable "Bar Coded Vote" BMDs provide hackers an avenue to rig elections through "Vote Swap Threat Model" fraud and are not suitable for use in elections for any voters.** Colorado recently announced that it will decertify all such systems after 2020 in its quest to be *"the safest place in the nation to cast a ballot"*.[ix]

Selection Summary Auditability Threat

"Selection Summary" BMDs which do not print a full ballot impair voter verifiability to the extent that they create a serious threat to auditability. These BMDs produce slips of paper with only the selections that the voter made. They do not include unselected candidates or referendum language.

While the ballot may *technically* be considered verifiable it requires the voter to memorize referendums, remember referendum language, recall the identity of unselected candidates and analyze the ballot for races that may have been accidentally skipped. In practice, this poses a significant burden for voters.

In a related report the National Academy of Sciences concluded:

> *"Unless a voter takes notes while voting, BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent."* [x]

Two dozen computer scientists further explained this in a 2019 letter to the Georgia Secretary of State:

> *"A post-election audit requires a valid source document, either marked directly by the voter or voter verified. Since voter verification of printed ballot summary cards (the source document) is sporadic and unreliable, elections conducted with most ballot marking devices are unauditable."* [xi]

A Rice University study conducted by Stephen Goggin and Michael Byrne found VVPAT systems that produce bar coded Selection Summaries have auditability issues. [xii] A recent Georgia Tech study of Tennessee voters conducted by Richard DeMillo, Robert Kadel and Marilyn Marks confirmed in significant detail that similar auditability issues clearly exist for the newer BMD technology.

The Georgia Tech study found voters do not adequately verify "Selection Summary" ballots or BMD ballots in general. Nearly half of the voters did not verify the selections on their ballots and those that did spent an average of less than four seconds to do so even though the ballot contained 18 races. After voting, voters who participated in the study were shown a ballot with several relatively significant errors and well over half believed the ballot they were shown was the correct ballot they voted while in the polling location. [xiii]

It may be unclear why voters were unwilling or unable to verify their votes in the Georgia Tech study:

- Were voters apathetic about verification since their votes were hidden in unverifiable barcodes?
- Was the Selection Summary too difficult to read and therefore mostly disregarded?
- Would full, transparent ballots have been subjected to the same fate?

However, the study made clear that this diminished verifiability creates a severe auditing issue that cannot be resolved by elections officials. Since voters are unwilling or unable to verify a 'Selection Summary', there is no original, voter-created source document that can be used for auditing purposes.

These studies and conclusions by scientists show that Selection Summaries cannot facilitate adequate auditing procedures and will thus nurture a 'Vote Swapping Threat Model' that can result in rigged elections. **Therefore, Selection Summaries are not suitable for conducting secure, auditable elections.**

BMD Malfunction Audit Threat

So far this paper has discussed inherent design flaws with normal functioning BMDs and their ballots. But what if a BMD of any kind malfunctions or is programmed to display incorrect race information to the voter in a manner that is difficult for the voter to notice? The burden is on the voter to detect the malfunction and communicate it to the poll manager even though the system does not generate any evidence the voter can present to prove there was a discrepancy. Professor Phillip Stark explained this problem in more detail in a letter sent to Georgia legislators:

> *"...widespread use of BMDs makes voters responsible for ensuring that BMDs function correctly. However, BMDs do not provide voters a way to demonstrate to poll workers or election officials that a BMD has malfunctioned, and the available evidence suggests that voters are not able to check BMDs effectively or reliably… This makes auditing elections that were conducted primarily using BMDs meaningless: an audit could easily confirm an incorrect outcome, because a BMD-generated paper trail is not a trustworthy record of voter intent."* [xiv]

In such a case, voters may be led to believe their printouts are correct after seeing incorrect race content shown on the BMD screen. Georgia Tech's Wenke Le explained the dilemma this would present to a voter in a 2019 report to the Georgia voting system commission he served:

> *"Further, many voters cannot detect the discrepancies between votes they have cast with a BMD and errors on the printouts, especially for "down-ballot" races. And some voters do not feel comfortable to speak up if they discover a discrepancy, perhaps because they think such a discrepancy should not have happened so it must be their own fault. Some, wanting to maintain their right to a secret ballot, hesitate to disclose to poll workers who they intended to vote for and the specifics of the error."* [xv]

A recent paper from Rice Professor Dan Wallach contends that auditing will detect any BMD problems:

> *"If a BMD is going to misbehave, the auditor will have a chance to catch it. And if any auditor, anywhere in the county, catches even one malicious machine in the act, the game is over. Call the police; we've got evidence of a serious crime."* [xvi]

While this scenario may be academically believable, it is not realistic from a practical perspective:

- Local police have little or no authority over state run and county run elections.
- If an auditor reported a machine producing malicious or incorrect results to election officials the officials would consider the machine to be an outlier and its results not evidence of any crime.
- In cases where there is evidence of a crime, election officials and state courts have resisted any investigation and attempted to conceal evidence from the general public. The "hold everything!" scenario rarely if ever is the way it works in the real world: the election proceeds and any such complaints are duly noted (or not) and buried with the passage of time.

The state of Georgia has a rich recent history to prove that voters cannot rely on election officials or courts to resolve security and auditability problems:

- In 2018, the Secretary of State (SOS) refused to open an investigation into why the Lt. Gov. Race had an excessive undervote rate that resulted in an estimated 127,000 missing votes.

- In 2019, a Cobb County Superior Court refused to allow voting machines to be forensically examined to determine what caused the 127,000 votes to potentially be lost.
- In 2013, the same court ruled that a candidate does not have a compelling reason to publicly view mail-in ballots from his own election even in the custody of county election officials.
- In 2016, when Logan Lamb found the ballot-building server to be exposed to the internet and vulnerable to hacking, the Center for Elections Systems (CES) failed to mitigate the vulnerability which was detected again in 2017.
- In 2017, when the central ballot-building server at CES was found to be exposed to internet hacking again for years, the SOS refused to open a forensic investigation to assess damage and mitigate any unrealized risks.
- In 2017, the SOS office hired a cybersecurity firm but directed its staff **NOT** to look at any elections related components including servers, scanners, voting machines and memory cards.
- In 2017, CES personnel allowed central elections servers to be wiped in violation of SOS data retention policies just after a voting system lawsuit was filed.
- In 2018, when the SOS moved CES ballot-building in house, they created a new ballot-building process that allows contractors to build ballots from their homes and transfer them over the internet to the SOS public server, where they are retrieved with a memory stick that is then inserted into the newly configured elections server.

The U.S. District Court was appalled when many of these findings were discovered in court evidence. Judge Amy Totenberg detailed her disgust in an order ruling Georgia DREs unconstitutional and banning them from future use. In that court case, plaintiffs presented 137 affidavits of elections problems. most of which went unresolved by officials. [xvii]

The inability and unwillingness of elections officials to resolve security and auditability problems is not limited to Georgia. The corruption of elections is too politically sensitive of a topic for many election officials throughout America. For example, South Carolina officials still contend that results from their unverifiable DREs were correct when the DREs made Alvin Greene a statewide 60-40% landslide winner over Judge Vic Rawl in the notorious 2010 U. S. Senate Democratic primary in which Rawl won the verifiable mail-in vote by a 55-45% margin. Greene was a virtual unknown who did not campaign or even have a web site. When Greene ran again in a subsequent state House primary he got only 37 votes (9%) in his own district. After presiding over perhaps the most controversial electronic election in U.S. history, the South Carolina Election Commission recently committed to buy another unverifiable voting system.

Professor Wallach correctly observes the political quandary: *"… it would be politically sensitive to declare that a cyberattack damaged an election and as such it had to be rerun…," b*ut in spite of the evidence, he surmises: *"…the likelihood of an emergency response mitigates against the risks of cyberattacks".*

Electronic voting history in America shows no likelihood of an emergency response. Voters cannot rely on such a remote possibility to protect their constitutional right to vote against risks of cyberattacks.

Dropped Race Threat Model

Even if one accepts the premise that voters and auditors can always detect a "Vote Swapping Threat Model" attack on a BMD by post-election paper ballot auditing, there is another type of threat model that voters can miss and **auditors are powerless to detect**. This attack involves manipulation of screen content displayed to the voter so the voter does not cast a complete or correct ballot as intended.

This type of malware employs a "Dropped Race Threat Model". If a BMD malfunctions or is programmed not to display a certain race or candidate to a voter, the voter may not be aware that the screen content is not correct and cast an inaccurate vote. Auditors have no practical mechanism to detect that type of BMD attack as they would when auditing blank pre-printed ballots before they are completed by voters.

Dropping a race from the display manifests itself in excessive undervotes for a race and would normally impact both candidates equally. However, a "Dropped Race Threat Model" can be programmed to selectively drop a race from the display under certain conditions known to the software operating within the BMD. These conditions could identify precincts or possibly even voters depending on their political leanings defined by their primary voting history. A target precinct list can be embedded in malware or read as a separate file. Thus, malware can change results of an election without actually swapping votes but simply reducing the chances voters of a particular political persuasion will vote in a given race.

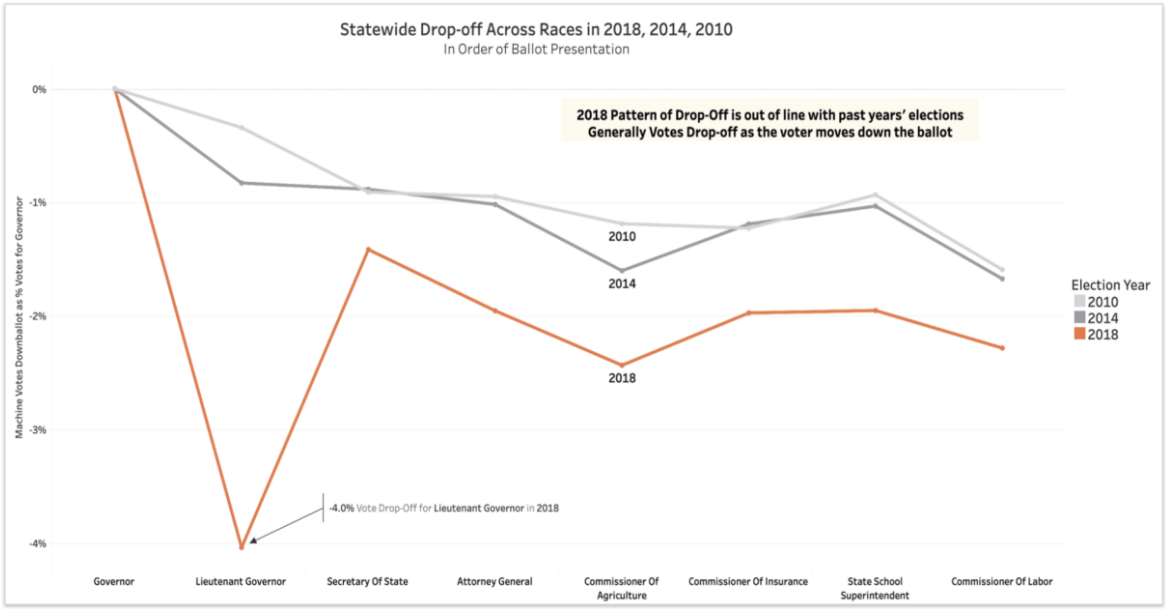
A "Dropped Race Threat Model" attack could be identified by a few voters who are familiar with races on a ballot. However, this type of attack can be programmed in a manner not easily detectable by an informed voter. Malware can suppress the race or candidate initially when the screen is displayed but then show the race or candidate if the voter spoils the ballot and starts over or returns from the ballot summary screen after recognizing a selection is missing. Even informed voters would think they made a mistake and overlooked the race initially since they have no mechanism to recall what they first saw.

Professor Wallach rightly calls for Live Audits of BMDs similar to parallel testing in an attempt to detect such problems. Under this procedure auditors or poll workers would produce test ballots and discard them during the day. But Professor Stark details a massive amount of permutations necessary for Live Audits to detect conditions that trigger vote alterations. Even if Live Audits were conducted frequently enough to detect BMD malware or a malfunction, (Ex: three times a day for each machine in each polling location), in practice, states are unwilling to commit to such a comprehensive auditing program. For example, Georgia admitted in U.S. District Court that it conducts a parallel test on only one of 27,000 DREs, a distant cry from what the state's own expert expected to ensure accurate elections. Live Audits are also vulnerable to error or fraud if test ballots are accidentally or intentionally scanned and cast.[xviii]

Virtually all post-election audits implemented for BMDs as of the time of this writing are limited in scope to auditing the paper ballot produced. **No practical audit procedures have yet to be developed to audit BMD content that is displayed to the voter.** Since auditors are powerless to stop it, the "Dropped Race Threat Model" is a more modern way to circumvent all current BMD audit procedures and rig elections without detection. **The impracticality of auditing BMD displayed content makes all BMDs inherently vulnerable to a "Dropped Race Threat Model" with little means to resolve the threat.**

A Real Life Dropped Race Undervote Anomaly

An example of a Dropped Race Threat Model that may have actually occurred is in the 2018 Georgia Lieutenant Governor's race between Republican Geoff Duncan and Democrat Sarah Riggs Amico. The race is significant because the Lieutenant Governor presides over the Georgia Senate and controls all legislation that passes through the body. That 2018 Georgia race produced the **greatest unexplained undervote anomaly by vote type in electronic voting history** as shown in this slide from a Coalition for Good Governance (CGG) report: [xix]



The strongly contested Lt. Gov. Race had a 4% undervote rate, nearly **triple** the 1.4% undervote rate of the next down ballot race for Secretary of State and more than **double** the 2% undervote for Attorney General Race and average undervote rate of other down ballot races.

Total 2018 Undervote by Office

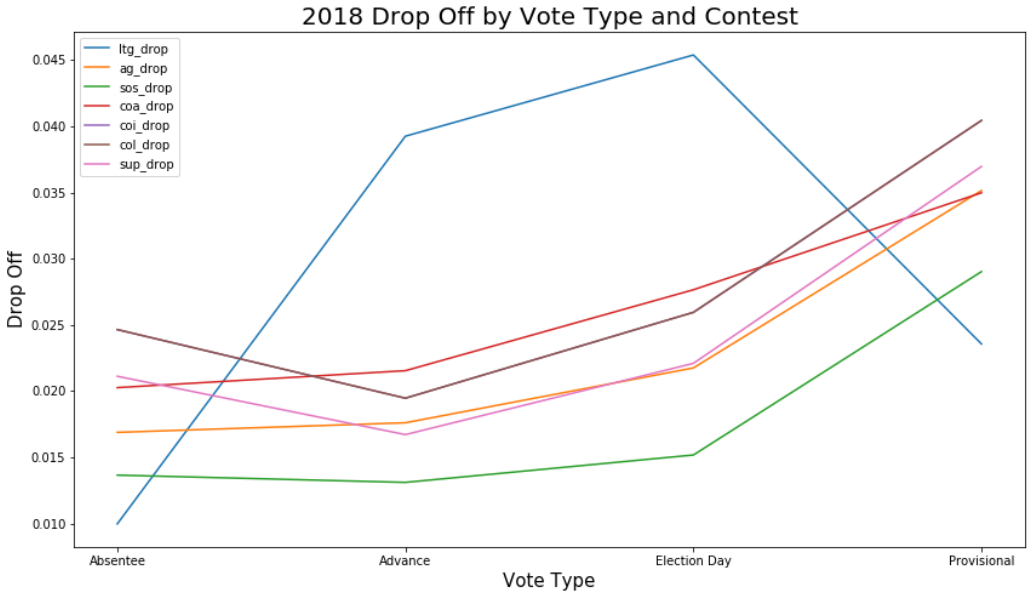
Office	2018	Under Vote	Drop Off vs Gov
Governor	3,939,328		
Lt. Governor	3,780,304	-159,024	4.0%
Secretary of State	3,883,594	-55,734	1.4%
Attorney General	3,862,370	-76,958	2.0%
Commissioner of Agriculture	3,843,480	-95,848	2.4%
Commissioner of Insurance	3,861,625	-77,703	2.0%
State School Superintendent	3,862,464	-76,864	2.0%
Commissioner of Labor	3,849,450	-89,878	2.3%

When compared historically to undervote rates for the same Lt. Gov. race, the 4% undervote rate was **five times** the 0.8% undervote rate for the same race in 2014 and **four times** the 1% undervote rate for the same race in 2010.

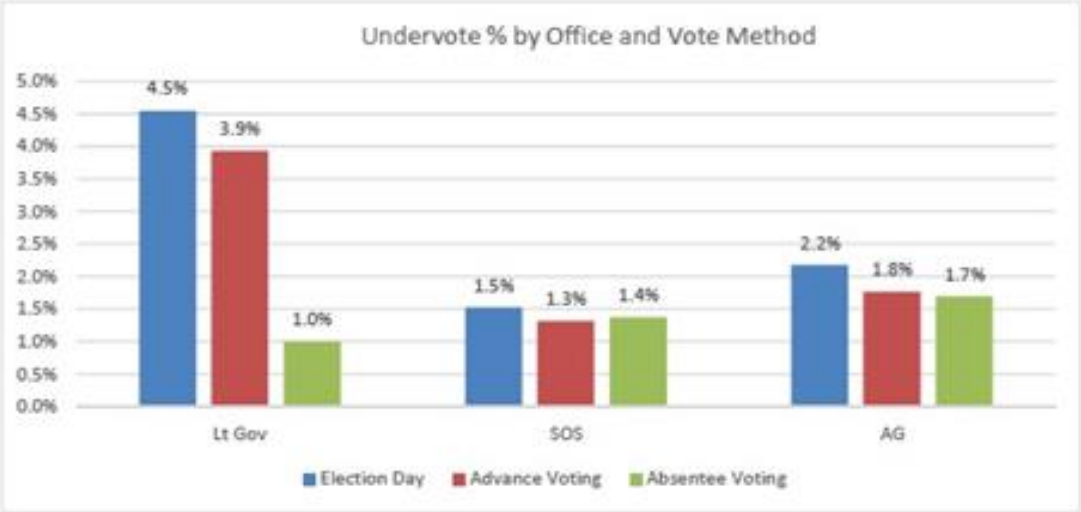
% Decrease in votes cast compared to that years gubernatorial contest

	2018	2014	2010	2006	2002
Lt. Governor	4.0%	0.8%	0.3%	1.2%	0.9%
Secretary of State	1.4%	0.9%	0.9%	2.8%	1.0%
Attorney General	2.0%	1.0%	0.9%	2.3%	2.8%
Commissioner of Agriculture	2.4%	1.6%	1.2%	1.8%	2.1%
Commissioner of Insurance	2.0%	1.2%	1.2%	2.4%	2.1%
State School Superintendent	2.0%	1.0%	0.9%	1.1%	1.2%
Commissioner of Labor	2.3%	1.7%	1.6%	3.1%	2.8%

But the exccessive undervote rate for the Lt. Gov. race **appeared only with votes cast on DREs**. The 1% verifiable mail-in undervote rate was normal and less than the 1.4% SOS mail-in undervote rate and the 1.7% Attorney General undervote rate.



Christopher Brill of Target Smart explained in his depositon for the U.S. District Court of Northern Georgia that ballot design was not a factor since the Lt. Gov. race appeared directly below the Governor race on the ballot. Brill affirmed there is no rational explanation for the excessive undervotes by vote type in the highly contested race. [xx]



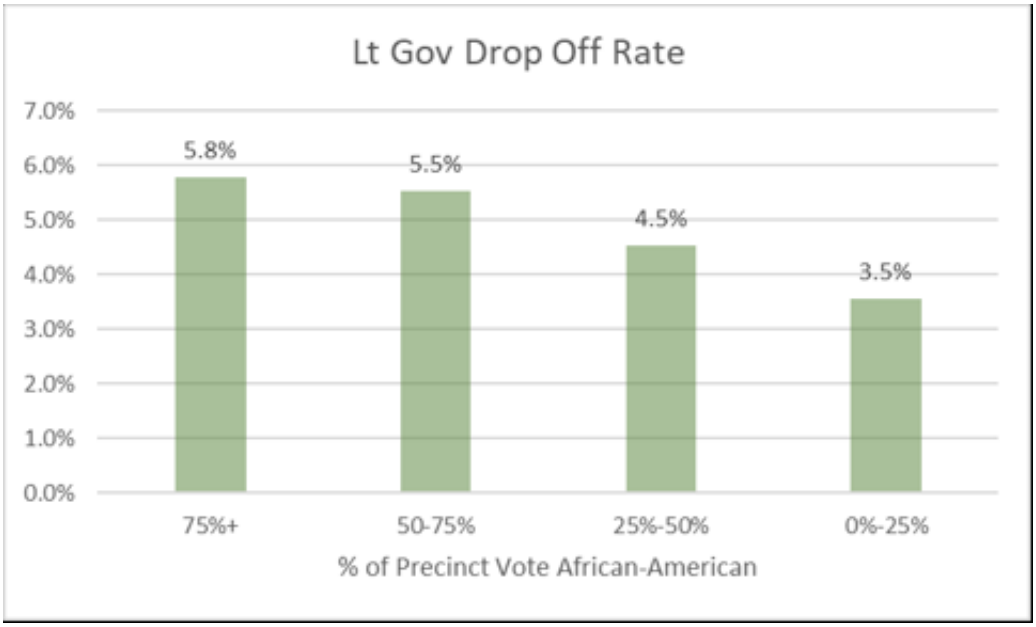
About 120,000 votes were lost based on the 1% verifiable mail-in undervote for the race. The coalition estimated that 127,000 votes were lost by the DREs based on the .8% previous Lt. Gov. Race and the historical undervote for the race.

Duncan won the contest over Amico by 123,000 votes. Duncan had previously won a controversial primary runoff by .3% or 1600 votes after trailing David Shafer 49-27% in the general Republican primary. Election watchers attribute that victory to over a million dollars of third party attack ads against David Shafer during the last weeks of the runoff.

Targeted Race Concealment

The General Election undervote did not appear to affect both Lt. Gov. candidates equally. Geoff Duncan retained a normal amount of all but about 1.35% of the Repubican votes for Governor Brian Kemp while Sarah Riggs Amico suffered a 4.94% drop off from the Democratic votes for gubernatorial candidate Stacey Abrams. Although there may be other reasons for this disparity, such as candidate popularity or election- impacting incidents no commonly known event occurred that could explain Amico's vote retention drop off other than the drop-off coming from the undervote anomaly.

A futher analysis by Brill in the CGG report revealed that at least 100 of 159 counties were impacted and the undervote impact was disproportional between the two candidates. Brill's analysis found the highest coorelation to the Lt. Gov. drop off rate is the percentage of African Americans for those affected precincts as iillustrated:



The analysis shows why Amico may have been disproportionally affected since African American voters impacted by the single race undervote anomaly tend to vote for candidates who are Democrats. The drop off cannot be explained by the racial difference between Abrams and Amico because Amico, SOS Candidate John Barrow and Attorney General candidate Charlie Bailey, all on the Democratic Party ticket, are Caucasian but Barrow and Bailey suffered no such drop off.

As of the time of this paper, a forensic analysis is still needed to establish a definitive assessment and to draw conclusions about the methods and circumstances that led to this unprecendented disproportional anomaly. Were precincts targeted for selective race concealment based on ethnicity of precinct voters? Could precincts have been targeted based on the primary voting history of their voters? Are there other factors that contributed to the undervote anomaly in that one race?

Although there are still unansweed questons about methods that may have been used, the evidence collected and presented in U.S. District Court so far indicates the possibility of a hacker targeting specific precints for manipulation of election results. At least two affidavits from voters indicated the race was only dropped on the initial ballot display screen but not when the voters returned from the summary screen to cast the missing vote. Thus, voters would be unlikely to notice the race if it only dissappeared from the initial display screen.

This type of targeted race concealment renders the “Dropped Race Threat Model” undetectble to any post election audit because there is no means to recall the BMD content displayed to voters.

Election Preparation Security Threat

BMDs and DREs can easily be rigged without detection to initiate "Vote Swapping" or "Dropped Race" threat models via a central election preparation system. BMDs have two event-triggered input pathways that are vulnerable to malware attacks. These events are:

- Receiving the ballot definition files delivered during election preparation.
- Receiving a ballot template ID with voter authorization at time of voting.

While both inputs may be feasible to hack, it is easier and less traceable to deliver a hacked file through the election preparation system to the BMD. Otherwise, a hacker must compromise the BMD, the voter registration system and the voter access mechanism that is typically a voter access memory card or voter-authorization bar code. While either is possible, the scope of this paper is limited to election preparation malware.

Election preparation malware can impact all elections conducted by all BMDs or DREs within the scope of the preparation delivery. Elections are typically prepped at the state or county level. Georgia operates statewide election preparation that is vulnerable to a **single point of attack.** If the central ballot-building server is exposed to the internet and receives malware, that malware could be automatically distributed to all counties and then to all BMDs or DREs as they are prepped for any election. The counties have no means to detect such malware and, once delivered, **the malware can continue to reside indefinitely on the infected servers or BMDs or both**. [xxi]

Wenke Le explained in his 2019 voting system commission report:

> *"In the context of election and voting systems, a ballot-marking device needs to be loaded with ballot data using a voting system memory card. The ballot data is formulated on another computer system, which is based on original data/documents, ---e.g., voter registration files and ballot programming files that at some point came from an Internet-facing system. Therefore, even though a BMD or voting machine is not directly connected to the Internet, it still is under the threat of cyberattacks from the Internet or by individuals who have direct access to the computers."*

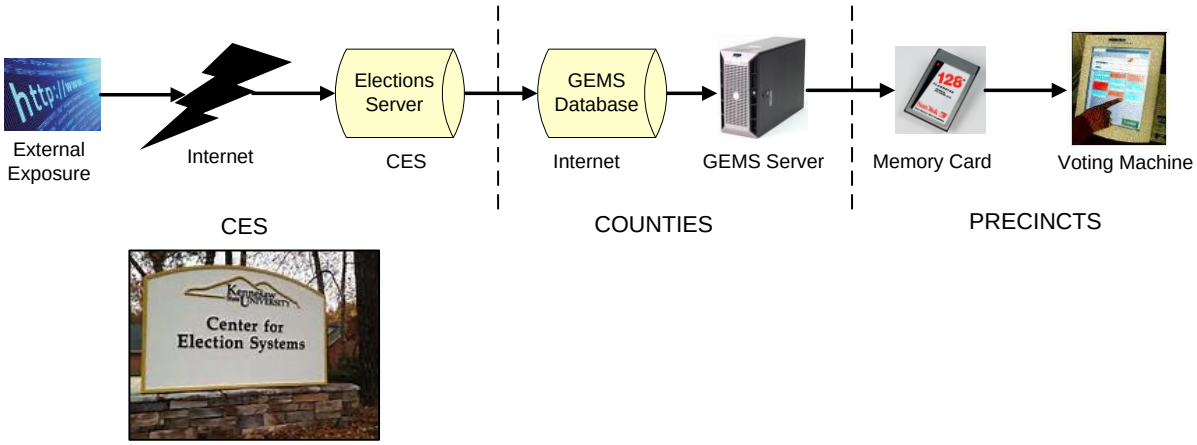
Elections officials throughout the country have falsely argued that voting machines are not connected to the internet simply because they are not connected while being used in an election. All voting machines are prepped from servers that receive files from other servers and in many cases these servers are connected to the internet at some point. Dr. Le further explained:

> *"… As long as a computer accepts input data from another device (software or hardware) that is or has been part of an Internet-connected network, it can still be hacked via the Internet."*

Elections officials have also falsely argued for years that a hacker must have physical access to a voting machine to hack it. On the contrary, malware can be delivered via a compromised ballot-building server to all servers and voting machines that are prepped from that server. **A hacker needs no physical access to any machine once the preparation server is exposed to the internet.**

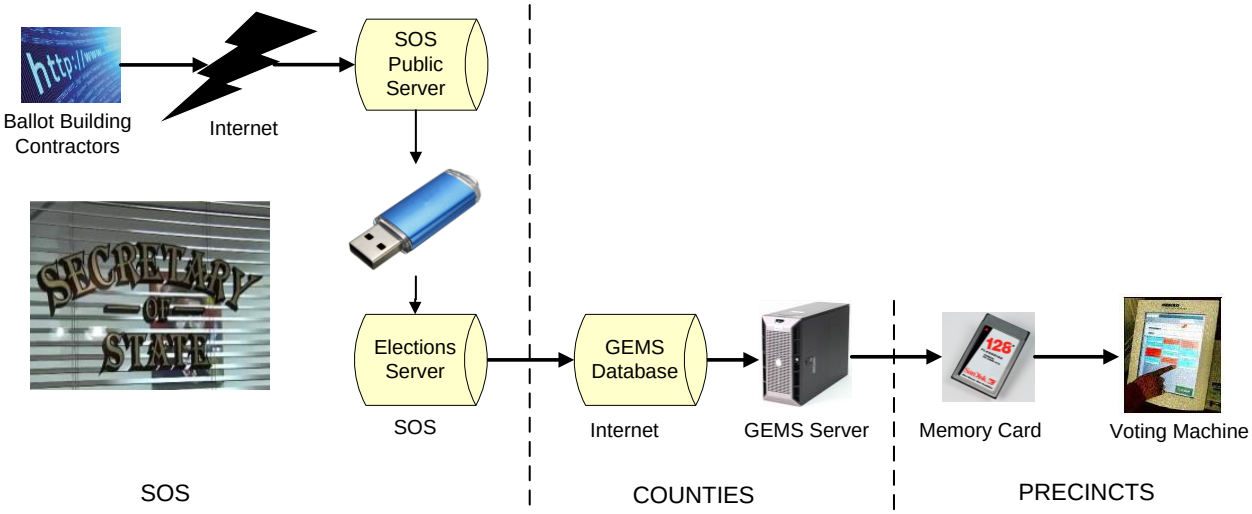
In the case of Georgia, the central ballot building server was found in 2016 to have been exposed to the internet for years and the county servers were never examined and disinfected after the discovery as explained in a previous **VoterGA audit**. In 2017, the exposure still existed, therefore, any election during the time period from about 2004 through 2017 could have been vulnerable to undetectable election rigging using the flow in the following diagram:

CES ELECTION PREPARATION PROCESS FLOW
2004 -2017



When the SOS took operational control of the ballot building servers from CES in 2018, the SOS office brought a similar process and key individuals in-house while failing to close the vulnerability again. This time the SOS employed contractors to build ballots *at home* with undefined security procedures and then deliver the ballots through a public-facing SOS server. From there the ballots were transferred into the central elections server using a memory stick as shown:

SOS ELECTION PREPARATION PROCESS FLOW
2018 -2019



.

These procedures illustrate that state election officials like those in Georgia are unwilling or unable to manage electronic voting systems of any type. Voters simply cannot rely on them to protect their constitutional right to vote from election rigging.

If a sophisticated attack was initiated in Georgia or another state, logic and accuracy testing cannot detect it. Malware can recognize whether a voting machine is in Election mode or Test mode and count differently depending on the operational mode of the machine. Dr. Ed Felten, Dr. Richard DeMillo as well as CES officials Britain Williams and Merle King have all confirmed this vulnerability in depositions and testimony for Georgia court cases.

Even if a BMD did not have mode switching, the malware can rely on internal clocks, voter volume, voting patterns or voter interaction speed to self-activate after bypassing detection during testing. The National Academies of Sciences Report summed up the situation in a single sentence:

> *"There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats."*

Furthermore, even if auditability could be employed to detect and mitigate the security risks of the "Vote Swapping Threat Model", there is no practical mechanism today to detect and mitigate the "Dropped Race Threat Model".

BMD Policy Conclusions

BMD Audit Weaknesses

Professor Wallach concluded in his paper:

> *"The risks of malware in current-generation BMDs are non-trivial, but they can be mitigated through human-centered ballot design, careful auditing procedures, and suitable election emergency laws"*

But Professor Wallach's paper did not consider the possibility of a Dropped Race Threat Model and how to mitigate it. The paper made no significant distinctions among the characteristics of BMDs, and how those characteristics further escalate security threats.

In contrast, this analysis argues that:

- Even with good human centered ballot design and the best BMD equipment, there are currently no post-election auditing procedures that can adequately mitigate BMD threats when BMDs are used for all voters.
- Live parallel audits require verification of too many permutations, voting machines and unpredictable circumstances for jurisdictions to willingly adopt.
- In practice, election rigging and election vulnerabilities are too politically sensitive for most states to conduct trustworthy audits and adopt such emergency laws as Wallach describes.

Professor Stark explains the live parallel audit dilemma:

1. *"The testers do not know which contest may be affected, or which candidate in those contests."*
2. *"The outcome of a small contest or a contest with a narrow margin can be changed by altering only a small fraction of votes—depending on actual voter preferences, an arbitrarily small fraction of votes."*
3. *"Malware or errors can be triggered by a vast number of combinations of many variables."*

There are just too many live parallel audit variables to ensure safe, secure electronic elections.

Professor Wallach concluded that:

> *"BMDs give us the security benefits of paper with the accessibility benefits of computers."*

In contrast, Professor Stark concludes:

> *"In practice, there are so many attack strategies (and possibilities for subtle bugs) that no reasonable amount of testing could guarantee even a modest chance of finding an outcome-changing problem."*

This analysis provides history and practical considerations that further confirm mass electronic voting on BMDs, has no means to mitigate all of the security threats that continue to jeopardize voters. It is obvious that hackers will exploit those threats and may have already.

Recommended BMD Evaluation Policies

To preserve the constitutional right of voters, jurisdictions must adopt protective policies for the acquisition and use of BMDs. Specific recommendations are:

- **Only stand-alone BMDs that produce full, transparent ballots should be acquired for use in the conduct of elections.**
  - BMDs that integrate scanners and tabulators into the same physical unit as the BMD are unsuitable for conducting elections because they provide a golden opportunity for hackers to alter ballots without detection ;
  - Systems that accumulate votes that BMDs s embed in bar codes not verifiable to the voter are unsuitable for conducting elections because they greatly increase the risk of undetectable election rigging;
  - BMDs that produce selection summaries are unsuitable for conducting election because they are inadequate in protecting privacy of disabled voters and establishing a proper audit trail for other any voter and are unsuitable to conduct elections for all voters.

- **BMDs must be limited to disabled voters to minimize the risk of undetectable election rigging and ensure it can be properly mitigated.**
  - **There is no post-election procedure that can audit what a BMD displays to each voter.**
    - BMDs remove the original voter-created source document necessary to establish a proper audit trail.
    - The burden to detect BMD malfunctions is left squarely on the shoulders of the voters, not election officials who should be responsible for that activity.
    - Voters do not have the means to determine if a BMD displayed races correctly to them and have no evidence to convince election officials if it malfunctions.
  - **It is not feasible to conduct adequate live parallel audits to ensure election integrity.**
    - A massive number of permutations must be tested in a live parallel audit environment to ensure the integrity of an election.
    - Jurisdictions are unwilling to commit the resources necessary to conduct the comprehensive live parallel audits that would be necessary.
    - Jurisdictions seem unwilling to accept the risk of having live test ballots accidentally or intentionally included in live election results.
  - **Voters cannot depend on election officials to conduct proper audits**
    - Audits identify problems only after an election is conducted and may require a new election as corrective action which has proven to be politically unpalatable and subject to legal challenge.
    - Election officials have historically been unwilling to investigate and resolve election problems or even reveal them when discovered. [GA, SC, OH]
    - The Election officials' top priority of conducting smooth, uneventful elections conflicts with auditing priorities of ensuring the accuracy of an election by revealing, investigating and resolving problems
    - Jurisdictions continue to ignore expert advice and purchase unverifiable voting equipment or systems that pose severe auditing problems despite having no procedures to mitigate the threats

BMD Legal Aspects

There is a growing consensus for these types of BMD policies among computer scientists, election integrity advocates and academic experts. While some jurisdictions make good faith efforts to adopt secure, verifiable and auditable systems others ignore expert warnings and are beginning to spend millions of taxpayer dollars to acquire the most vulnerable types of BMD systems. These unresolved security threats are beginning to drive citizen unrest and legal cases against certain BMD acquisitions.

A U.S. District Court has already banned paperless DREs in Georgia for 2020 and beyond because their lack of verifiability, auditability and recount capabilities impair the constitutional right to vote of the citizens. In addition, the court found many other reasons that the state is sorely lacking in the ability to securely manage electronic elections. The court ruling was so comprehensive that it minimized the possibility of appeal and will likely set a benchmark for other cases.

Both sets of plaintiffs in the case amended or supplemented their complaints to challenge Georgia's planned 2020 implementation of an unverifiable BMD system that tabulates hidden votes embedded in bar codes. The U.S. District court now has two briefs before it to consider banning those BMDs as well. If the court makes a decision in that matter, the decision will also likely have landmark implications for other jurisdictions. [xxii] [xxiii]

Jurisdictions that plan to acquire new voting systems should:

- Objectively consider established election integrity expert opinions and studies.
- Review the legal cases now pending before U.S. District Court.
- Incorporate verifiability, auditability, security, and privacy criteria into their evaluations.
- Establish public policy for the use of BMDs.
- Carefully assess the costs and benefits of BMD, BOD and HMPB systems

These steps are necessary to protect voters who have already suffered through nearly two decades of unverifiable, paperless DRE voting from further disenfranchisement.

Appendix

VOTERGA — **PROJECTED GEORGIA VOTING SYSTEM COSTS** — **Vendor Overview**

DEVICES & SOFTWARE	Min Price	Max Price	HAND MARKED PAPER BALLOTS # Devices	HAND MARKED PAPER BALLOTS Min $	HAND MARKED PAPER BALLOTS Max $	BALLOT ON DEMAND SYSTEMS # Devices	BALLOT ON DEMAND SYSTEMS Min $	BALLOT ON DEMAND SYSTEMS Max $	BALLOT MARKING DEVICES # Devices	BALLOT MARKING DEVICES Min $	BALLOT MARKING DEVICES Max $
Electronic Poll Book	$995	$1,200	7,095	$7,059,525	$8,514,000	7,095	$7,059,525	$8,514,000	7095	$7,059,525	$8,514,000
Ballot Marking Device	$3,500	$7,200	2,365	$8,277,500	$17,028,000	2,365	$8,277,500	$17,028,000	30,745	$107,607,500	$221,364,000
On Demand Ballot System	$4,500	$4,895	0	$0	$0	4,730	$21,285,000	$23,153,350	0	$0	$0
Precinct/County Scanner	$5,750	$7,900	4,890	$28,117,500	$38,631,000	4,890	$28,117,500	$38,631,000	4,890	$28,117,500	$38,631,000
County Hi Speed Scanner	$25,000	$111,500	160	$4,000,000	$17,840,000	160	$4,000,000	$17,840,000	160	$4,000,000	$17,840,000
County Tabulation Server	$17,954	$17,954	160	$2,872,640	$2,872,640	160	$2,872,640	$2,872,640	160	$2,872,640	$2,872,640
County Training Days	$1,700	$2,000	480	$816,000	$960,000	480	$816,000	$960,000	480	$816,000	$960,000
	PURCHASE COSTS			$51,143,165	$85,845,640		$72,428,165	$108,998,990		$150,473,165	$290,181,640
	MINIMUM SAVINGS			$99,330,000			$78,045,000				
Poll Book Licensing Fee	$51	$51	7,095	$361,845	$361,845	7,095	$361,845	$361,845	7,095	$361,845	$361,845
Ballot Marking Device License	$65	$228	2,365	$153,725	$539,220	2,365	$153,725	$539,220	30,745	$1,998,425	$7,009,860
Ballot on Demand Licenses	$195	$390		$0	$0	4,730	$922,350	$1,844,700		$0	$0
Precinct Scanner License	$80	$228	4,730	$378,400	$1,078,440	4,730	$378,400	$1,078,440	4,730	$378,400	$1,078,440
Hi Speed Scanner License	$1,575	$2,575	15	$23,625	$38,625	15	$23,625	$38,625	15	$23,625	$38,625
County Election Mgmt License	$4,082	$7,500	160	$653,120	$1,200,000	160	$653,120	$1,200,000	160	$653,120	$1,200,000
Poll Book Maintenance	$51	$51	7,095	$361,845	$361,845	7,095	$361,845	$361,845	7,095	$361,845	$361,845
Ballot Marking Device maint.	$75	$235	2,365	$177,375	$555,775	2,365	$177,375	$555,775	30,745	$2,305,875	$7,225,075
Ballot on Demand Maint.	$195	$390		$0	$0	4,730	$922,350	$1,844,700		$0	$0
Precinct Scanner Maint	$110	$135	4,730	$520,300	$638,550	4,730	$520,300	$638,550	4,730	$520,300	$638,550
Hi Speed Scanner Maint	$1,500	$1,895	15	$22,500	$28,425	15	$22,500	$28,425	15	$22,500	$28,425
County Election Mgmt Maint.	$4,082	$7,500	160	$653,120	$1,200,000	160	$653,120	$1,200,000	160	$653,120	$1,200,000
Per Device Ballot Testing	$50	$100	14,365	$718,250	$1,436,500	18,920	$946,000	$1,892,000	42,745	$2,137,250	$4,274,500
Per Device Storage/Transport	$75	$100	14,365	$1,077,375	$1,436,500	18,920	$1,419,000	$1,892,000	42,745	$3,205,875	$4,274,500
Avg Maint. & License Increase			14,365	$291,610	$701,371	19,095	$387,629	$932,313	42,745	$867,724	$2,087,025
County Election Support Avg	$4,500	$4,675	272	$1,224,000	$1,271,600	272	$1,224,000	$1,271,600	272	$1,224,000	$1,271,600
Ongoing County Training Days	$1,700	$2,000	320	$544,000	$640,000	320	$544,000	$640,000	320	$544,000	$640,000
Auditing Per Precinct Average	$100	$250	4,021	$402,050	$1,005,125	4,021	$402,050	$1,005,125	4,021	$402,050	$1,005,125
Per Paper Ballot Printing	$0.20	$0.45	0	$0	$0	5,567,803	$1,113,561	$2,505,511	5,567,803	$1,113,561	$2,505,511
Per Paper Ballot Pre-Printing	$0.28	$0.55	6,681,363	$1,870,782	$3,674,750	0	$0	$0	0	$0	$0
Pre Print Admin/Distribution	$0.10	$0.20	6,681,363	$668,136	$1,336,273	0	$0	$0	0	$0	$0
	ANNUAL EXPENSES			$10,102,057	$17,504,843		$11,186,794	$19,830,675		$16,773,514	$35,200,926
	MINIMUM SAVINGS			$6,671,457			$5,586,720				

See Next Page for Variables and Assumptions

DRE = Direct Recording Electronic System — BOD = Ballot on Demand System — BMD = Electronic Ballot Marking Device

VOTERGA — **PROJECTED GEORGIA VOTING SYSTEM COSTS** — **Vendor Overview**

Variables	Count
# Counties + SOS:	160
#Precincts:	2,365
Registered Voters	6,550,356
Average Annual Elections	1.70
Average Tunrout	50.00%
Annual Average Demand Ballots	5,567,803
Pre-Printed Excess Factor	20%
Scanners Per Precinct	2
Poll Books Per Precinct	3
BOD Systems Per BOD Precinct	2
BMDs Per HMPB Precinct	1
BMDs Per BMD Precinct	13
Annual Maint/License Increase	3.50%
Maint & Licensing Term Years	10
High Scan Volume Counties	15
Initial County Training Days	3
Ongoing County Training Days	2

Pre printed paper ballots marked by hands of voters or by assistive technology for disabled voters

Ballot on Demand printers that print ballots for voters to hand mark as they check in at any polling location

Ballot Marking Devices used by all voters to mark and print paper ballot selections

ALL BALLOTS ARE INSERTED INTO THE SCANNER BY THE VOTER AND ACCUMULATED ELECTRONICALLY

Assumptions

1.- Estimates include new pollbook system that integrates with electronic BMDs or BOD systems
2.- At least 10% more BMDs than DREs are needed in BMD estimate for voter ballot printing time
3.- Estimates include tabulation and ballot building server for each county and one central site
4.- Minimum and maximum costs are derived from vendor responses received and released to date
5.- Spreadsheet accounts for cost differences in types of voting systems but not all election costs
6.- At least one BMD is needed at each precinct in HMPB estimate to provide assistive technology
7.- At least two BOD systems are needed at each precinct in BOD estimate in case of malfunction

xxiv xxv

TOPIC	PRE PRINTED HAND MARKED PAPER BALLOTS w/ BMDs for ADA VOTERS (HMPB)	BALLOT ON DEMAND PRINTING FOR HAND MARKED BALLOTS (BOD)	ELECTRONIC BALLOT MARKING DEVICES for ALL VOTERS (BMD)
	Advantages	Advantages	Advantages
Acceptance	Recommended by all cybersecurity experts, election integrity advocates, computer scientists Preferred by majority of voters at meetings and by independent poll	Acceptable to voters, election directors, cybersecurity experts and computer scientists	Preferred by majority of county election directors
Audits	Ballot is auditable as original source document created personally by voter independently of system	Ballot is auditable as original source document created personally by voter independently of system	
Costs	Saves Georgians $100+ million **initially** over BMDs Saves Georgians $7+ million **annually** over BMDs Saves Georgians $20+ million on **initially** over BODs	Saves Georgians $80+ million **initially** over BMDs Saves Georgians $7+ million **annually** over BMDs	
Errors		Programmatic selection of correct ballot style	Programmatic selection of correct ballot style Prevention of overvote, immediate notification of undervote
Printing		Reduced ballot pre-print quantity	Reduced ballot pre-print quantity
Vulnerability	Ballot mark not vulnerble to hack	Ballot mark not vulnerable to hack	
Dependency	No device dependence to cast vote	No device dependence to cast vote	
Reliability	Proven process used by most states		
Liability	Likely to resolve federal lawsuit and prevent further suits	Likely to resolve federal lawsuit and prevent further suits	
	Disadvantages	Disadvantages	Disadvantages
Audits			Cannot be meaningfully audited according to 24 computer scientists, Risk Limiting Audit inventor
Costs		Costs Georgians about $20 million more **initially** over HMPB	Costs Georgians $100+ million more **initially** over HMPBs Costs Georgians $7+ million more **annually** over HMPBs Costs Georgians $80+ million more **initially** over BODs Costs Georgians $7+ million more **annually** over BODs 20 year bond means Georgia will pay twice as long as shelf life of system
Errors	Detection of overvote, undervote at scan time instead of upon race Manual selection of correct ballot style by poll workers	Detection of overvote or undervote at scan time instead of upon race	
Printing	Requires extra ballot preprint costs and administrative control		
Vulnerability		Ballot style selection could be vulnerable to hacking	BMD display, ballots and style selection are vulnerable to hacking
Dependency			Depends upon machine to cast vote
Reliability			No statewide BMD implementation has ever been attempted
Liability			Not likely to resolve federal lawsuits and puts Georgia at risk of more

xxvi

References

[i] Letter to Assistant Secretary Michael Barnes, Garland Favorito

[ii] *"Security Analysis of the Diebold AccuVote-TS Voting Machine"* - Feldman, Halderman, Felten

[iii] *Favorito v. Handel Deposition* – Professor Britain Williams

[iv] *"Ballot Marking Devices (BMDs) Cannot Assure the Will of Voter"* - Appel, DeMillo, Stark

[v] *"Design Flaw in Dominion ImageCast Evolution Voting Machine"*- Appel

[vi] "*Serious Design Flaw in ESS ExpressVote Touchscreen: "permission to cheat"* – Appel

[vii] *"On the notion of software independence in voting systems"* - Rivest and Wack

[viii] *"Ohio Election Workers Convicted of Manipulating 2004 U.S. Presidential Recount*"– International Herald Tribune

[ix] *"Colorado Secretary of State Announces Initiative to Remove QR Codes from Ballots"* – Colorado Dept. of State

[x] *"Securing the Vote"* – National Academy of Sciences

[xi] *"Experts Letter to SAFE Commission"* – 24 various Computer scientists

[xii] *An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots*" – Goggin, Byrne

[xiii] *"A Quantitative Analysis of Voters Memories if Their Ballots"*– DeMillo, Kadel, Marks

[xiv] *"Ballot-marking devices (BMDs) are not secure election technology"* (letter) – Stark

[xv] *"Addendum to Basic Security Requirements for Voting Systems"* – Le

[xvi] *"On the Security of Ballot Marking Devices"* – *Wallach*

[xvii] Curling V. Raffensperger Civil Action No. 1:17-CV-2989-AT, U.S. District Court, Northern Georgia

[xviii] *"There is no Reliable Way to Detect Hacked Ballot-Marking Devices"* – Stark

[xix] *"Georgia's 127,000 Missing Votes"* – Coalition for Good Governance

[xx] *Curling v. Raffensperger Deposition* – Christopher Brill

[xxi] *Georgia Elections Data Destruction Audit* – VoterGA

[xxii] Curling v. Raffensperger, Coalition Plaintiffs' Supplemental Complaint – Attorney Bruce Brown

[xxiii] Curling v. Raffensperger, Curling Plaintiffs' Amended Complaint – Morrison & Foerster

Voting System Evaluation Tools

[xxiv] Voting System Cost Estimator

[xxv] Sample Incumbent Georgia Vendor Cost Sheet

[xxvi] BMD, BOD, HMPB Comparison Overview